INTERACTIVE SECURITY

COMPLYING WITH PRIVACY SHIELD AND GDPR: *A MUST FOR DOING INTERNATIONAL DIGITAL BUSINESS TODAY*

To combat the explosion of digital malefactors aiming to steal and disrupt, Privacy Shield and the General Data Protection Regulation have emerged to protect data and international business.

Author: Shawn C Corrigan
President/Managing Partner
Interactive Security
www.intactsec.com
267.824.2500

Despite what the media may think, the interconnected global economy is nothing new. The economic collapse of the early 1770s played a key role in helping to kick off the American Revolution. Destructive breaches into data security are as old as intelligence services, which also date back centuries. Over the centuries, nation-states have created international agreements and rules to protect the interests of their people in trade and information.

The digital era has introduced new threats to data and the trade that depends upon it. Malevolent forces from individuals to organized crime, to terrorist groups and rogue nation-states have discovered great benefits from breaking into hidden data troves. They can make illicit money, disrupt an operation, or find other ways to sow problems.

To combat the explosion of digital malefactors aiming to steal and disrupt, Privacy Shield and the General Data Protection Regulation have emerged to protect data and international business. They represent two very different, but complementary and even symbiotic measures to protect personal data flowing between the European Union and Switzerland on one hand and the United States on the other.

What Is Privacy Shield?

Privacy Shield represents a United States government effort to work with partners in Europe in designing a system of protocols where companies and organizations agree to meet standards of data protection. One of the Privacy Shield programs covers United States and European trade while another specifically protects US and Swiss economic exchanges. The International Trade Administration, an office under the US Department of Commerce, administers Privacy Shield.

Privacy Shield ensures that information and trade that includes personal data coming from European Union member countries and Switzerland will have protection. It helps to resolve differences between European and American mandates and standards of personal data protection.

Conforming to the US Freedom Act, membership in Privacy Shield is voluntary. Any company seeking registration must prove that they meet the standards set by the US Department of Commerce. Once on the list, companies must comply with the strict data protection standards.

The US Department of Commerce will place approved companies and organizations who self-certify on a list which is made publicly available. Each registrant must re-certify annually. Any registrant can voluntarily remove themselves from the Privacy Shield list, however voluntary or involuntary removal will prevent the company or organization from receiving personal data from European Union member states or Switzerland.

What Is the General Data Protection Requirement?

Six years ago, the European Union set out to construct data protection programs to counter the growing threat to personal information from malefactors across the globe. The centerpiece of this effort lies in creation of the General Data Protection Requirement, or GDPR, which came into force in May 2018.

The GDPR replaces the old European Data Protection Directive that applied data protection standards to organizations operating within the European Union. In the advent of personal data being processed across the global as a common practice, the EU had to extend its reach. The GDPR covers any company or organization that,

while providing a product or a service, processes personal data of citizens of EU member states, even if done as a free service.

Organizations that monitor individuals' online behavior must also comply. While most will understand how this could apply to entities like Google or Facebook, it also includes organizations with even a peripheral connection to personal data of European Union member citizens. This includes customers, employees, and end users.

The aim of the GDPR lies in helping individuals gain more control over what happens to their personal data. At the same time, it seeks to simplify regulations to help companies and other organizations comply with the new laws.

The GDPR is much more complex than Privacy Shield and includes legal details that Americans may find odd. One example being that if multiple entities are involved in processing and controlling information are involved in an incident producing compensable damages, the GDPR requires each party involved to pay full compensation.

Running afoul of the GDPR could be costly over and above compensation to those whose personal data is affected by data breaches. Under the law, companies could have to pay twenty million Euros or four percent of their global revenues for violations.

These new laws and regulations are intended to ensure that companies and other organizations collect data under strict and legal conditions. Companies and organizations must also follow strict data protection protocols that consider data privacy a right.

Separate and Overlapping, But Different Legal Requirements

Privacy Shield and the GDPR both have the same general aim, to protect personal data collected while doing business or providing a service. They perform this function in very different ways, but adherence to both standards is necessary.

The GDPR and Privacy Shield have a symbiotic legal relationship. State and federal personal data protection laws are considered insufficient by the European Union, but the EU has no enforcement mechanism outside of its jurisdiction. When a US company successfully registers under Privacy Shield, it has a legal obligation to comply with the stricter regulatory standard and can also interact with EU member citizens.

While the EU has no direct enforcement mechanism within the US, Privacy Shield provides forums where Europeans can register complaints as well as enforcement mechanisms. Europeans can appeal to an ombudsman at the Department of State or a special arbitration panel.

Also, registration with Privacy Shield constitutes a legally binding promise to continually comply with its standards. The Federal Trade Commission, or in some cases, the Department of Transportation can sanction companies or organizations that run afoul of data protection standards.

Organizations that transfer personal data involving citizens of European Union member states must not stop at compliance with Privacy Shield. They must also perform their due diligence in making sure that they comply with guidelines specific to GDPR and stay current with any new developments.

Compliance with Privacy Shield and GDPR a Must for International Business

While the global economy and its impact has shaped the world for centuries, data and international exchanges have never been more vulnerable. Yesterday's pirates took to the high seas to steal valuables; today all they need is an internet connection and a keyboard.

A theft of personal data can unravel and destroy an innocent person's life without warning.

Protecting personal data is not solely national or international law; organizations should treat it as a sacred trust and stress adherence to standards proven to protect it.

The bad guys are out there and continue to perfect attacking data each day. These include criminals, organized crime, terrorists, and rogue nation-states. None of these malefactors will respect the privacy of those whose data they steal. Organizations need to do their due diligence to protect personal data - registration and compliance with Privacy Shield and GDPR represents a strong first step toward solid information protection.

About Interactive Security

Since 2007 Interactive Security, Inc. has been at the forefront of providing industry leading expert information technology security services to clients across the globe - focused on IT Security Auditing & Compliance.

Our team is comprised of highly skilled industry certified professionals with diverse experience serving technology consulting firms and enterprise security departments. We serve a broad base of clients and industries including the payment card industry, finance, legal, healthcare, education, government, restaurant and hospitality.

Our clients and partners choose Interactive Security because of our uncommon ability to provide expert custom IT security services that exceed both technical and business expectations.

We pride ourselves on Making ***IT COMPLIANCE OBTAINABLE, SIMPLE AND AFFORDABLE.***

*Vulnerability / Penetration Assessments * Application Security * BCP/DR Planning * PCI DSS * HIPAA * HiTRUST * ISO 27001-27002 * ISO 31000 * NACHA ACH * FEDRAMP * FISMA/NIST * GDPR * Privacy Shield*